Group Policies

Group Policy is a method for configuring the computers in your forest. The policies can be applied to the **Computer** or to the **User**. Group Policy has nothing to do with Groups. They are completely separated components.
An instance of a Group Policy is usually called Group Policy Object (GPO). A GPO can be used to, for example, set the screensaver on a computer, specify which control panel options should be available to the user, which programs should be showed in the start menu. The settings can then be applied to set of user or computer objects by linking the GPO with a OU or a Domain.

A GPO can be applied to a Site, Domain and OU. It cannot be applied to a container (such as **Builtin** or **Users**).

Group Policies are extremly powerful, and a misconfigured GPO can shutdown the operation of an company. It is also extremly granular. You can make detailed changes applied to only a few objects in a specific OU.

There are some best practices that are good to keep in mind when using GPOs:

- Keep user and computer settings in different GPOs.
- Apply the smallest number of GPOs to solve the problem.
- Try to avoid duplicating settings in differnt GPOs.

Two GPOs are create by default when you first install Active Directory:

- Default Domain Policy - Basically only sets the Password and lockout policy.
- Default Domain Controllers Policy - Set security configurations for the Domain Controllers.

It is common to not edit the default policies and instead create new ones. If you mess things up, you can just remove those policies and you always have the default ones clean.

Started GPOs

It is common to create template GPOs, these are called Starter GPOs. These can be used if you need to create multiple GPOs that share a lot of configurations, but differ on some.

Working with GPOs

GPOs are managed from the "Group Policy Management Console" (GPMC or just GPM).

In broad strokes a GPO allows for computer configuration and user configurations.

- Computer configuration - applied to the computer irrespective of the user who logged on.
- User configuration - applied to the user irrespective of the computer they're using.

Both of these configurations (User and computer) have Policies and Preference settings.

Policies for user configuration are placed in the HKEY_CURRENT_USER (HKCU) area of the Registry, while those for computer configurations are placed in the HKEY_LOCAL_MACHINE (HKLM) area.

Policies

Policies contain settings that have been available since Group Policy was introduced in Windows 2000. These are thousands of settings that can be done. They are divided up in three groups: Software settings, Windows settings, and Administrative Template.

Both User and Computer configurations have the same main categories (Software, Windows, Administrative Template). But the differe. So some configurations are only available for Computers, and other are only Available for Users. In fact, the Computer Configuration branch has 1644 settings available, whereas the User Configuration branch has 1453 settings available.

Computer policies are the following:

- Software settings - Used to automatically install programs. You configure a UNC path to a `.msi` and that package will be installed the assigned computer, or the computer where a user log in.
- Windows settings - DNS, Startup/shutdown scripts, Deploy printer, and Security - firewall rules, trusted root certificate, password options, audit logs.
- Administrative Template - This is where the majority of configurations are. Not really use the difference between Windows settings and Administrative Template.

Preferences

Preferences are what they sound like: they are what is prefered. This means that they can be overridden by a user. It is just a preference, not a law. Before prefences was included in Windows 2008 many configurations were configured through logon-scripts. Things that are configured with Preferences are: - Drive and printer mappings - Power scheme management - File and folder management, including creating and deleting files and folders - Applications - Network share management - Scheduled tasks (This is where the GPP-vuln is found - see (Passwords in Group Policy Preferences) [../active_directory_privilege_escalation/passwords_in_group_policy_preferences]) - Services - Also suceptible to GPP-vuln.

It is possible, and probably a good idea, to disable all User configurations if a GPO is suppose to be applied only to Computers, and vice verse. This can be done in the

Applying GPOs

The process of applying a GPO to a specific container (Site, Domain, OU) is usually called linking. If you haev a GPO but it is not linked to any container then it doesnt really do anything. You can link and unlink a GPO. You usually do this but opening the GPMC and then either click on a container and create a new GPO. Or create a GPO in "Group Policy Objects" and then drag the GPO to the container you want to link it to.

It usually takes up to 90 minutes for the computers in the domain to poll for the new GPOs, this can be bypassed by runnign the command `gpupdate /force`.

Security updates cna take up to 16 hours.
Domain Controllers update GPOs every 5 minutes.

Order of applying GPOs

1. Site
2. Domain
3. OU
4. Nested OU

If multiple GPOs have made the same GPO change, the lowest in the chain (closes to the leaf) is the one that will be applied.

BLocking and overriding

Blocknig inheritance

GPOs are inherited by OUs. So if one OU has a GPO linked to it, the GPO will be applied to all the sub-OUs. The GPO is therefore inherited. If you do not want sub-OUs to inherit GPOs you can configure that OU to block inheritance.

Overriding / Enforced

If an OU has blocked the inheritance it is still possible to override that setting by configuring the GPO above to be Enforced. If it is enforced the below OUs can't block inheritance.

Filtering

Group

It is possible to filter whom the GPO will be applied to further. This cna be done with the Filter options. You can add Groups, and only the users belonging to that group will have the GPO applied. The default is "Authenticated users".

WMI Filter

You can also filter whom the GPO will be applied to by using WMI filters. With WMI you can filter on computer disk space, OS version, etc